TRAFIKKDATA OVER BRUK AV ELEKTRONISK KOMMUNIKASJON

Politiets adgang til å bruke disse ved bekjempelsen av kriminalitet

Kandidatnr: 302

Veileder: Lee A Bygrave

Leveringsfrist: 25.04.03

Til sammen 13600 ord

(* se http://www.jus.uio.no/sekr/studieinformasjon/fagsider/spesialoppgave/)

Innholdsfortegnelse

1 Innledning

1.1 Oppgavens tema

Den teknologiske utvikling har medført at vi lever i et samfunn der vi flere ganger daglig legger igjen elektroniske spor[1] som gjør det mulig å kartlegge vår hverdag stadig mer detaljert. Bruk av Internett, telefon, bankkort, køfribrikker, adgangskort o l genererer forskjellige opplysninger om brukeren. Fra politiets ståsted innebærer dette en stor fordel, da det gjør det lettere å oppspore gjerningspersoner som har benyttet slike midler. Særlig opplysninger om bruk av elektronisk kommunikasjon er nyttige i en slik sammenheng. Slike opplysninger kalles trafikkdata[2].

For at disse opplysningene skal kunne brukes som ledd i etterforskning av straffbart forhold, må de oppbevares ut over den tid bruken tar. Hva som lagres, vil variere med de enkelte tilbydere av elektronisk kommunikasjon og de regler som er gitt for slik lagring. Videre må politiet ha adgang til å benytte opplysningene.

Behovet for effektive etterforskningsmetoder kan imidlertid komme i strid med personvernhensyn. Det pågår en internasjonal debatt om dette tema[3], hvor det særlig er uenighet om hvor lenge opplysningene skal lagres.

Denne oppgaven redegjør for de hensyn som taler for og mot lagring av trafikkdata, og hvordan dette er regulert i gjeldende rett. Det er særlig bruk av telefon og Internett som blir behandlet her. Det må likevel fremheves at reglene i stor grad gjelder generelt, for alle former for elektroniske kommunikasjon.

---

[1] Begrepet ble først brukt av Mestad i "Elektroniske spor. Nye perspektiv på personvern" Complex 1986

[2] Se nærmere definisjon under avsnitt 1.4.

[3] Se Allitch og Manansian

1.2 Problemstillinger

En forutsetning for at trafikkdata over bruk av telefon og Internett skal kunne brukes ved etterforskning av et straffbart forhold, er at disse opplysningene lagres, slik at politiet kan få tilgang til de når det er nødvendig. Bruk av trafikkdata klassifiseres som et tvangsmiddel i straffeprosessen. Det utgjør for den som utsettes for det et inngrep av en slik art at det etter legalitetsprinsippet er nødvendig med hjemmel i lov.

Jeg vil i det følgende først se om det oppstilles en plikt til å lagre de ulike typer av opplysninger. Dersom det ikke er en plikt til å lagre opplysningene, blir spørsmålet om det er adgang til det, og herunder hvilke vilkår som i så fall stilles. Deretter vil jeg behandle reglene om politiets tilgang til de opplysninger som måtte være lagret. Relevante problemstillinger herunder er hvilke vilkår som stilles for tilgang.

Spørsmålene reguleres av flere regelsett. Rettslige problemstillinger knyttet til disse reises fortløpende i avhandlingen.

1.3 Avgrensning

I tillegg til trafikkdata over bruk av elektronisk kommunikasjon, kan bl a opplysninger om innholdet i kommunikasjonen tenkes å være interessant i etterforskningssammenheng. Det vil imidlertid falle utenfor rammen for denne oppgaven å behandle disse.

Oppgaven konsentreres om hvilke muligheter politiet og påtalemyndighetene i Norge har til å benytte trafikkdata i etterforskningen. Samarbeid over landegrensene og utveksling av informasjon mellom landene blir ikke behandlet her.

Norge er forpliktet av flere internasjonale konvensjoner på dette området. Av disse blir Europarådets konvensjon om cybercrime[4] og EMK art 8 behandlet i det følgende. Også SP art 17 kunne vært relevant i denne sammenheng, men blir ikke behandlet her. Dette fordi det forligger mer rettspraksis knyttet til EMK art 8, og fordi de to regelverk i all hovedsak regulerer spørsmålet likt.

[4] Jeg velger å ikke oversette begrepet ”cybercrime” i det følgende.

Reglene om trafikkdata brukt som bevis behandles ikke; det sentrale i denne oppgaven er hvordan disse opplysningene kan bidra på etterforskningsstadiet. Det vil også falle utenfor denne oppgavens rammer å behandle spørsmål knyttet til kryptering[5].

1.4 Begrepsdefinisjoner

IKT-kriminalitet: Kriminalitet som knytter seg til bruk av informasjons- og kommunikasjonsteknologi. Begrepet omfatter nye kriminalitetsformer som datainnbrudd og skadeverk via kommunikasjonsnett, men også all kriminalitet hvor man tar beslag i elektroniske bevis[6].

Elektroniske spor[7] er opplysninger som automatisk registreres elektronisk når man bruker kort ved betaling av varer eller tjenester, passerer en bomring med køfribrikke, bruker mobiltelefon eller lignende. Disse sporene gir informasjon om hvilke aktiviteter man har bedrevet. Et slikt spor inneholder minst en opplysning som kan kobles til en person, f eks kode, kundenummer, telefonnummer, bilnummer, personnummer, navn eller adresse.

Data er informasjon som er presentert på en måte som gjør at den kan tolkes, overføres eller behandles[8].

Trafikkdata er opplysninger som genereres ved bruk av elektroniske kommunikasjonsmidler og som angir hvilke elektroniske kommunikasjonsutstyr; telefoner, mobiltelefoner, personsøkere, datamaskiner osv, som har vært i kontakt med hverandre. Opplysningene angir kommunikasjonens opprinnelse, endested, rute, tidspunkt, dato, størrelse, og varighet[9]

IP-adresse: Hver datamaskin som er pålogget Internettet har en unik adresse, og alle elektroniske impulser som overføres i forbindelse med kommunikasjon adresseres med

---

[6] Jf Sunde (2000).

[7] Mestad, jf note 1.

[8] Wagle og Ødegård s 498

[9] Jf Europarådets konvensjon om cybercrime art 1 d.

en slik adresse, slik at de blir styrt til riktig server. Det er denne adressen som sørger for at e-post kommer til riktig adressat eller at man finner riktig web-side[10].

Øvrige begrep som benyttes i oppgaven, defineres underveis

1.5 Den videre fremstilling

Avhandlingen faller i tre hoveddeler. I kapittel 2 redegjøres det for rettskilder og metode som er brukt i avhandlingen. Deretter gjøres det i kapittel 3 rede for de ulike hensyn som gjør seg gjeldende. Det gjeldende regelverk som regulerer de angitte problemstillingene behandles i kapittel 4. Her behandles først nasjonal lovgivning, deretter de internasjonale rettskilder. I kapittel 5 knyttes noen kommentarer til oppgaven.

[10] Sunde (2000).

2 Rettskilder og metode

Bruk av trafikkdata reguleres både av nasjonal lovgivning og av internasjonale konvensjoner og direktiver som Norge er bundet av. Da metoden er noe ulik for disse to grupper av rettskilder, redegjør jeg først for de norske rettskilder og metoden som er benyttet her, deretter tilsvarende for de internasjonale konvensjoner.

2.1 Norsk lovgivning

Redegjørelsen av de norske rettskildene bygger på vanlig juridisk metode, etter gjeldende rettskildelære[11]. De relevante lover i denne sammenheng, er personopplysningsloven, teleloven og straffeprosessloven. Disse lovene regulerer ulike sider av spørsmålet om lagring av trafikkdata og tilgang til disse, og det foreligger ingen motstrid mellom disse som gjør det nødvendig å ta stilling til motstrids- og harmoniseringsspørsmål. Utgangspunktet for forståelsen er tatt i de aktuelle bestemmelsenes ordlyd. I det følgende gis en oversikt over de rettskildefaktorene som har betydning for tolkingen av de ulike lovene. Juridisk teori er benyttet som en rettskildefaktor[12].

2.1.1 Personopplysningsloven

Lov av 14. april 2000 nr 31 om behandling av personopplysninger[13] regulerer lagring av trafikkdata, dersom disse omfattes av begrepet personopplysninger. Forarbeider til personopplysningsloven er NOU 1997:19 og Ot prp nr 92 (1998-99). Videre vil konsesjonspraksis fra Datatilsynet bli brukt i redegjørelsen. Datatilsynet er et uavhengig forvaltningsorgan administrativt underordnet Kongen og departementet, jf pol § 42. Praksis fra dette organet vil derfor ha lik vekt som vanlig forvaltningsorgan[14]. Av juridisk teori, er Johansen m fl og Bygrave og Schartum sentrale kilder. Bygrave 1997 har vært benyttet for Datatilsynets praksis. Det foreligger ingen relevant rettspraksis på området.

---

[11] Se f eks Eckhoff

[12] Jf Eckhoff Helgesen kap 1.

[13] Omtales heretter som pol.

[14] Se f eks Eckhoff, Torstein: Forvaltningsrett (1997) kapittel 12.

2.1.2 Teleloven

Lov 23. juni 1995 nr 39 om telekommunikasjon[15] regulerer all telekommunikasjonsvirksomhet. I denne sammenheng er det først og fremst taushetspliktbestemmelsen i § 9-3 som er relevante. Aktuelle forarbeider her er Ot prp nr 31 (1997-1998). Videre bidrar en høyesterettsavgjørelse[16] til å klargjøre bestemmelsens innhold.. Av juridisk teori har Bing m fl vært lagt til grunn. Teleloven skal erstattes og oppheves av ny lov om elektronisk kommunikasjon, se nedenfor.

2.1.3 Ny lov om elektronisk kommunikasjon

I ot prp nr 58 (2002-2003) foreslås ny lov om elektronisk kommunikasjon (ekomloven), som skal erstatte dagens telelov. Lovforslaget implementerer relevante EU- og EØS-regler. Det tas sikte på at loven skal tre i kraft 25. juli 2003.

2.1.4 Straffeprosessloven

Lov av 22. mai nr 25 1981 om rettergangsmåten i straffesaker[17] regulerer politiets tilgang til trafikkdata. Det foreligger flere høyesterettsavgjørelser som er relevante for tolkingen av disse bestemmelsene. De relevante forarbeider til straffeprosessloven er i denne sammenheng NOU 1997:15, Ot prp nr 64 (1998-1999) og Innst O nr 3 (1999-2000). Av juridisk teori er og Bjerke og Keiseruds kommentarutgave lagt til grunn.

2.2 Internasjonale rettskilder

De internasjonale rettskilder som blir behandlet i denne oppgaven, er Europarådets Convention on Cybercrime, EMK art 8 og EU-direktiv 02/58. Nedenfor redegjøres det kort om internasjonale konvensjoners stilling i norsk rett generelt. Deretter følger rettskildemessige særtrekk som gjelder for EMK og EU-direktivet.

---

[15] Heretter telel.

[16] Rt 1999 s 1944. Denne behandles nedenfor under kap 6.

[17] Heretter strpl.

2.2.1 Generelt om internasjonale rettskilders stilling i norsk rett

De internasjonale rettskildene vil ha betydning ved tolking av de norske lovbestemmelsene, i tillegg til den egenbetydning de har der er de stiller strengere krav enn hva som følger av norsk lov. Det kan her oppstå spørsmål om hvorvidt norsk lovgivning er i samsvar med de internasjonale forpliktelser. Det er derfor nødvendig å si noe om hva som skjer ved evt motstrid mellom en internasjonal rettskilde og norsk lovgivning, og generelt om hvilken vekt de internasjonale forpliktelsene har i norsk rett.

Etter den tradisjonelle oppfatning følger Norge et dualistisk system, dvs at for at en ratifisert traktat skal bli del av norsk rett, kreves en særlig gjennomføringsrettsakt. Dette kan skje på tre måter; ved inkorporasjon (det vedtas en norsk regel som henviser til traktaten), transformasjon (norske regler utformes slik at de er i samsvar med traktaten) eller konstatering av normharmoni (det foretas en sammenligning som viser at det ikke er påkrevd med lovendringer i norsk rett). Dette er imidlertid kun et utgangspunkt. Det har lenge vært den rådende oppfatning at det gjelder et presumsjonsprinsipp som går ut på at norsk intern rett formodes å være i samsvar med folkeretten[18]. Spørsmålet er ikke om folkeretten har relevans, men hvilken vekt den skal ha.

Spørsmålet om internasjonale konvensjoners stilling i norsk rett reguleres også av straffeprosessloven § 4:

> Lovens regler gjelder med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat.

Denne begrensningen gjelder generelt for de regler som må anses fastslått som folkerettslig sedvanerett, men også de regler som følger av traktater og konvensjoner som er bindende for Norge. Uttrykket ”begrensninger” må her tolkes utvidende, slik at det også omfatter plikter som følger av konvensjonene[19].

---

[18] Jf Eckhoff v Helgesen kapittel 12.

[19] Jf Bjerke og Keiserud s 39

2.2.2 EMK art 8

EMK er implementert som norsk lov ved lov av 21. mai nr 30 1999 om styrking av menneskerettigheter (menneskerettsloven). Menneskerettsloven § 3 gir følgende bestemmelse om motstrid:

> Bestemmelsene i konvensjoner og protokoller som er nevnt i § 2 skal ved motstrid gå foran bestemmelser i annen lovgivning.

Disse konvensjonene gis med dette en sterkere stilling enn "vanlig" norsk lov. Ved innføringen av menneskerettsloven ble det diskutert om internasjonale konvensjoner skulle gis grunnlovs rang. Dette ble ikke gjennomført. De internasjonale konvensjonene som ble innført som norsk lov ved menneskerettsloven har dermed en mellomstilling mellom en vanlig lovbestemmelse og en grunnlovsbestemmelse("semi-konstitusjonell status)[20].

2.2.3 EU-direktiv

Norges forpliktelse til å gjennomføre relevante EU- og EØS regler følger av EØS-avtalen art 102. De aktuelle EU-direktiv i denne sammenhengen er direktiv 95/46/EF (om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger), direktiv 97/67/EF (om behandling av personopplysninger og beskyttelse av privatlivets fred innenfor telesektoren) og direktiv 02/58/EF (om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor). 97/67/EF erstattes og oppheves av 02/58/EF[21]

2.3 Reelle hensyn

Hensynet til personvernet og til behovet for effektive etterforskningsmidler er de mest sentrale ved tolkingen av alle disse rettskilder. Det redegjøres for disse i kapittel 3. det fremgår underveis hvilke kilder som er benyttet ved fremstillingene.

---

[20] Jf Helgesen i Eckhoff s 325.

[21] Se nedenfor under avsnitt 4.3.1.

3 De motstridende hensyn

Jeg vil i dette kapittelet gi en innføring i de to sett av hovedhensyn som står i mot hverandre ved vurderingen av lagring av trafikkdata. Dette er på den ene siden samfunnets behov for å bekjempe kriminalitet, og på den annen side hensynet til personvern. Personvern kan iakttas fra flere vinkler, og det er til dels omfattende teori på området. Redegjørelsen for dette vil derfor bli noe mer omfattende enn avsnittet som omhandler behovet for effektive etterforskningsmidler.

3.1 Personvern

3.1.1 Innledning

Personvernhensyn er anerkjent i flere internasjonale konvensjoner, blant annet er det tatt med i SP art 17 og i EMK art 8. Begrepet personvern brukes ofte uten at det gis en nærmere definisjon av hva det innebærer. I flere av de lover som behandles nedenfor, er ivaretakelse av personvernhensyn angitt som ett av flere formål, jf f eks telel § 1-3 h og pol § 1. Andre steder anføres personvernhensyn som ett moment i en interesseavveining for om ulike tiltak skal iverksettes. Eksempel på dette finner vi i diskusjonen om innføring av regler om kommunikasjonskontroll[22]. Det er derfor nødvendig å si noe om hva personvern er. I det følgende blir det først kort gjort rede for den tradisjonelle fremstillingen av personvern i norsk rett (punkt 3.1.2). Deretter gis en fremstilling av et nyere og mer omfattende bidrag til personvernteorien (punkt 3.1.3). I punkt 3.1.4 følger en redegjørelse for personvern angitt som et sett grunnleggende prinsipper, fordi disse er mer anvendelige som et analyseverktøy. Til slutt behandles hvilke aspekter ved personvern som særlig blir berørt ved behandling av trafikkdata (punkt 3.1.5).

3.1.2 Hva er personvern?

Det er vanskelig å gi en eksakt definisjon på personvern. De fleste assosierer begrepet med stikkord som ”personlig integritet” og ”privatlivets fred”[23]. Det er slik begrepet benyttes i dagligtalen. Denne betydningen av begrepet er også lagt til grunn i flere

[22] Jf NOU 1997:15

[23] Se Bygrave 2002 kapittel 7 for en redegjørelse av de verdier personvernet omfatter.

juridiske verk, og også Høyesterett refererer til disse verdiene når det snakker om personvern.

Det kan også anlegges ulike perspektiv for å klargjøre begrepet. Personvern kan iakttas fra flere ulike vinkler; det integritetsfokuserte personvern, det maktfokuserte personvern og det beslutningsfokuserte personvern[24]. Det integritetsfokuserte personvern legger vekt på individets behov for å ha kontroll over opplysninger av personlig karakter om seg selv. Dette innebærer også retten til å være i fred fra andre. Perspektivet kan deles inn i ulike typer integritet; territorial, kroppslig, psykisk, kommunikasjonsintegritet og informasjonsintegritet[25]. Det maktfokuserte personvern tar hensyn til at et stort informasjonstilfang kan være opphav til makt, både i private og offentlige sammenhenger. Dette perspektivet foranledninger politiske og filosofiske vurderinger om hvilken grad av kontroll som er ønskelig i et samfunn. Det beslutningsfokuserte personvern legger vekt på at opplysninger ofte er grunnlag for å treffe beslutninger om enkeltpersoner. Det fokuseres her på at slike beslutninger må treffes på måter som er egnet for å sikre at resultatet blir riktig og rettferdig.

I Norge har personvern tradisjonelt blitt forklart ved hjelp av et sett interesser som de enkelte borgere antas å være opptatt av. Disse er kun oppstilt som en antakelse; det er ikke foretatt systematiske undersøkelser blant "mannen i gata" som gjør at man kan konstatere disse interessene, de er mer et teoretisk utgangspunkt. Knut Selmer og Dag Ragnar Blekelid utviklet tidlig på 1970-tallet en modell hvor personvernet blir beskrevet ved hjelp av to sett av interesser; individuelle og kollektive. Disse to hovedgruppene av interesser er igjen delt opp i flere under-interesser. De individuelle interessene er angitt ved stikkordene diskresjon, fullstendighet, innsyn og privatlivets fred. De kollektive interessene kan oppsummeres ved stikkordene en borgervennlig forvaltning, et robust samfunn og et begrenset overvåkningsnivå[26]. Denne modellen har siden blitt revidert og utviklet i takt med endringer samfunnet og utvikling i teknologien. Flere forfattere har gitt sine bidrag til dette.

---

[24] Se NOU 1997:19 s 21-23.

[25] Bygrave og Schartum kapittel 2 s 8 flg.

[26] Dag Ragnar Blekelid og Knut S Selmer: Data og personvern, Universitetsforlaget 1977

Den teknologiske utviklingen og de enorme muligheter for innsamling og lagring av personopplysninger den innebærer, har ført til at perspektivet på personvern har blitt dreid mot elektronisk behandling av personopplysninger. Personvernets kjerneområde angis derfor nå som de regler som regulerer behandling av personopplysninger. Personvern kan etter dette forstås som summen av lover, normer og tiltak som ivaretar den enkeltes interesse i at personopplysninger tilfredsstiller visse kvalitetskrav og at de ikke behandles på en utilbørlig måte[27].

3.1.3 En ny utgave av interessemodellen

Lee A. Bygrave og Dag Wiese Schartum gir en fremstilling av personvern som kombinerer og supplerer de tidligere bidragene til interesseteorien. De tar utgangspunkt i personvern som et ideal som i rendyrket form er uoppnåelig, men som ivaretas ved hjelp visse interesser. De oppstiller fem hovedinteresser som igjen konkretiseres i krav som interessene begrunner. Kravene kan igjen munne ut i tiltak som kan fremme personvernet. Disse interessene er:
interessen i å bestemme over tilgangen til opplysninger om egen person
interessen i innsyn og kunnskap
interessen i opplysnings- og behandlingskvalitet
interessen i forholdsmessig kontroll
interessen i brukervennlig behandling

Interessen i å bestemme over tilgangen til opplysninger om egen person
Utgangspunkt for denne interessen er at menneskene har selvbestemmelsesrett over opplysninger om seg selv. Dette bygger på to grunnleggende verdier i vårt samfunn; menneskets autonomi og verdighet. Det er imidlertid flere unntak fra dette utgangspunktet om at mennesket fritt kan disponere over opplysninger om seg selv. I et demokratisk samfunn er det flere eksempler på at denne friheten må innskrenkes, og at opplysninger samles inn og behandles uten vedkommendes samtykke. Dette kan følge av lovbestemte forpliktelser, f eks betaling av skatt, men frivilligheten kan også

[27] Wiik Johannesen s 22-23

begrenses av praktiske årsaker. I vårt moderne samfunn er vi avhengig av å gi fra oss opplysninger i utallige dagligdagse situasjoner. Den reelle frivilligheten er derfor meget begrenset. Det er like fullt oppstilt som en interesse, og den ivaretar særlig to viktige aspekter. Det første er på individuelt nivå; det kan være av stor betydning for individet at de har en reell mulighet til å velge hvem som skal ha tilgang til opplysninger om dem. Behandling av opplysninger med grunnlag i tvang eller urettmessig tilgang bør derfor unngås. På kollektivt nivå gjenspeiler interessen et ønske om at samfunnet skal organiseres og innrettes slik at den enkelte selv kan velge i hvilken grad hun vil gi fra seg personopplysninger.

Interessen i å kontrollere tilgangen til opplysninger om egen person konkretiseres i tre krav:

Krav om etablert tillitsforhold
Dette gjenspeiler behovet for at behandling av personopplysninger i størst mulig grad skal bygge på et tillitsforhold mellom den registrerte og den behandlingsansvarlige. Dette uttrykkes ofte i lovgivningen som et krav om at det i visse tilfeller må innhentes et frivillig og informert samtykke for at behandling av personopplysninger skal være lovlig, jf pol §§ 8 og 9.

Krav om konfidensialitet
Dette kravet innebærer i utgangspunktet at spredningen av opplysninger om den registrerte skal begrenses til det omfang og på den måte som den registrerte selv ønsker eller ville ha ønsket. Dette kravet kan oppfylles på minst fire måter; ved å gjøre avgivelse av personinformasjon frivillig for den enkelte, ved å beskytte personinformasjonen slik at ikke uvedkommende får tilgang til den dersom noen gjør forsøk på å tilegne seg den, ved å legge begrensninger på aktiv videregivelse av personinformasjon (taushetspliktbestemmelser), ved å legge begrensninger på måten videregivelse kan skje.

Krav om beskyttet privatliv
Også denne interessen forutsetter at opplysninger om private og personlige forhold ikke spres til andre. Dette vernet er videre enn det som følger av konfidensialitetskravet, ved

at det retter seg mot den kollektive enhet der privatlivet leves. Det inkluderer dermed familien og husstanden ellers. Videre er behovet for fravær av uønskede fredsforstyrrelser og oppmerksomhet omfattet i dette kravet.

Interessen i innsyn og kunnskap

Dette er en grunnleggende personverninteresse som tar hensyn til at individet trenger kunnskap om de forhold som har betydning for hvordan behandling av opplysninger om dem skjer. Slik kunnskap er nødvendig for å vite om ens lovbestemte rettigheter ivaretas, og om de behandlingsansvarlige oppfyller sine pålagte plikter.
Denne interessen blir ivaretatt ved hjelp av krav om rettsinformasjon, krav om generelt innsyn, krav om individuelt innsyn og krav om begrunnelse.

Interessen i opplysnings- og behandlingskvalitet

Denne interessen angår kvaliteten på de opplysninger som samles inn og den behandling som blir foretatt. Kvalitet blir her brukt som en betegnelse på hvor egnet opplysningene og behandlingen er i forhold til de aktuelle bruksformål. Interessen konkretiseres i visse kvalitetskrav.

Interessen i forholdsmessig kontroll

Begrepet kontroll er her brukt om ulike måter for innsamling av informasjon for å vurdere om folks handlinger er i samsvar med rettslige og sosiale handlingsnormer. Utgangspunktet er at kontroll med om lovlige fattede vedtak og andre lovlige avgjørelser overholdes, er legitimt og nødvendig i et demokratisk samfunn. Det dreier seg her om kontroll både innen privat og offentlig sektor, selv om grunnlaget for utøvelse av kontroll er forskjellig i de to tilfeller.

Interessen i forholdsmessig kontroll ivaretas ved følgende krav til forholdsmessighet: Forholdsmessighet mellom veiledning og kontroll, mellom forhåndskontroll og etterkontroll, mellom kontroll til de registrertes gunst og til deres ugunst og mellom ekstern og intern kontroll.

Interessen i brukervennlig behandling

Denne interessen konkretiseres med krav om hvordan forholdet mellom den registrerte og den behandlingsansvarlige skal være. Dette er av betydning for å bygge opp det tillitsforhold som ble omtalt ovenfor. Interessen oppfylles ved at det stilles krav om lydhørhet, forståelighet, uhindret dialog og driftsstabilitet

3.1.4 Grunnleggende prinsipper for behandling av personopplysninger

I andre europeiske land er personvernet ofte forklart ved hjelp av et sett med grunnleggende prinsipper. Disse prinsippene er i en viss grad utledet fra OECDs retningslinjer for personvern, Europarådets konvensjon om personvern, og EUs personverndirektiv. Dette utgjør en alternativ fremstillingsmåte til interesseteorien, og kan særlig være til nytte ved analyse av personvernspørsmål. Prinsippene har normativ betydning ved at de i noen tilfeller er innført som rettsregler. Videre fungerer de som retningslinjer ved vedtakelse av ny lovgivning og ved interesseavveininger som tilsynsmyndighetene foretar[28]. I det følgende redegjøres det for de mest sentrale og allment aksepterte prinsippene.

Rettferdighet og rettmessighet

Prinsippet om at personopplysninger skal behandles på en rettferdig og rettmessig måte (”fair and lawful”) er det mest grunnleggende prinsippet. De øvrige prinsippene er innbakt i dette og utledes herfra. Rettmessighetsprinsippet omfatter blant annet krav om at den behandlingsansvarlige skal ta i betraktning og ha respekt for den registrertes interesser og rimelige forventninger. Prinsippet innebærer et krav om forholdsmessighet for de inngrep som behandlingen eventuelt medfører. Videre skal behandlingen være gjennomsiktig og forståelig for den registrerte.

Minimalitet

Essensen i dette prinsippet er at opplysninger bare skal samles inn i den grad det er påkrevd for å oppnå formålet med innsamlingen og den videre behandlingen av

[28] Bygrave og Schartum kapittel 3 s 13.

opplysningene. Så snart det ikke lenger er nødvendig å oppbevare opplysningene for det formål de ble samlet inn for eller senere er brukt til, skal de slettes eller anonymiseres.

Formålsbestemthet[29]

Prinsippet om formålsbestemthet fastslår at personopplysninger ikke kan brukes til andre formål enn det de opprinnelig ble samlet inn for. Dette innebærer at formålet med behandlingen skal angis presist, og at formålet må være legitimt. Formålet må videre være i tråd med den behandlingsansvarliges ordinære, lovlige virksomhet.

Opplysningskvalitet

Dette prinsippet reiser krav om at personopplysninger skal være korrekte i forhold til det de skal representere. Prinsippet krever videre at opplysningene er "relevante, adekvate og fullstendige i forhold til deres bruksformål."

Medbestemmelse

Prinsippet om medbestemmelsesrett oppstiller krav om at den registrerte skal kunne delta og ha en viss innflytelse over andres behandling av opplysninger om vedkommende. Den behandlingsansvarlige skal som følge av dette aktivt informere den registrerte om sine behandlingsoperasjoner. Videre innebærer prinsippet at opplysningene i størst mulig grad skal samles inn direkte fra den det gjelder. Prinsippet bygger på et utgangspunkt om at individene selv bestemmer over når andre skal kunne samle inn opplysninger om dem, og hva opplysningene skal brukes til senere. De registrerte skal dessuten kunne kreve at uriktige, ufullstendige og ulovlig innsamlede opplysninger rettes eller slettes.

Informasjonssikkerhet

Den behandlingsansvarlige pålegges etter dette prinsippet å etablere tiltak for å sikre uautorisert eller utilsiktet tilgang, videregivelse, endring og /eller sletting av personopplysninger.

[29] Se Lenth s 11.

Sensitivitet

Dette prinsippet bygger på at visse opplysninger om en person er av en slik art at de krever strengere regulering enn "vanlige" personopplysninger. Dette gjelder først og fremst opplysninger om personers helse, seksualitet, rase eller etnisk bakgrunn, og politiske, religiøse eller filosofiske overbevisninger. Også medlemskap i visse organisasjoner, f eks fagforeninger, er ansett å omfattes av denne kategorien.

Bygrave[30] opererer også med "disclosure limitation" som eget prinsipp. Dette er ikke oppstilt som eget prinsipp i alle internasjonale reguleringer, men inngår i prinsippet om rettferdighet og rettmessighet og i prinsippet om formålsbestemthet. Det sentrale er at databehandleres adgang til å gi personopplysninger videre til tredjeparter er begrenset ved at det kun kan skje under visse vilkår.

I tillegg til prinsippene nevnt hittil, er også et prinsipp om anonymitet i ferd med å slå gjennom[31].

3.1.5 Aspekter ved personvern som særlig berøres ved lagring av trafikkdata

Det kan oppstå et motsetningsforhold mellom politiets ønske om og behov for å benytte trafikkdata til å oppklare lovbrudd og hensynet til personvern. I det følgende skisseres kort hvilke problemstillinger lagring av trafikkdata reiser i forhold til personvern.
Det forutsettes i det følgende at politiet får tilgang til trafikkdata på de måter som regelverket åpner for, slik at det ikke oppstår spørsmål om tilgangens rettmessighet, jf legalitetsprinsippet.

Prinsippet om formålsbestemthet

Trafikkdata lagres for å danne grunnlag for riktig fakturering. Det er derfor på det rene at bruk av disse opplysningene som middel for å oppklare lovbrudd i utgangspunktet

[30] Bygrave 2002 s 67

[31] Bygrave og Schartum

ikke er i samsvar med det opprinnelige formålet[32]. Dersom det pålegges lagringsplikt utover det tidsrom som teletjenestetilbyderne ønsket, er også dette i strid med formålet. Kravet til formålsbestemthet innebærer også at formålet med behandlingen skal angis på en presis måte. Dersom trafikkdata skal brukes av politiet i forbindelse med etterforskning, fordrer dette prinsippet at formålet med lagring av trafikkdata må utvides til også å omfatte etterforskning.

Minimumsprinsippet

Opplysningene skal etter dette slettes eller anonymiseres så snart de ikke lengre er nødvendige ut fra det de ble innsamlet for eller senere er brukt til. Dette prinsippet innebærer at dersom det skal innføres lagringsplikt utover det tidsrom som er nødvendig for f eks fakturering, må formålet med lagringen endres.

Opplysningskvalitet

Bruk av trafikkdata som etterforskningsmetode kan gi opplysninger som ikke er korrekte i forhold til det de pretenderer å si noe om . Politiet bør derfor være opptatt av kvaliteten på de opplysninger de får tilgang til.

Interessen i å bestemme i tilgangen til opplysninger om egen person

Dette kan være i strid med kravet til konfidensialitet; at spredningen av opplysninger om den registrerte skal begrenses til det omfang som vedkommende selv ønsker eller ville ha ønsket. Også kravet om etablert tillitsforhold berøres.

Kontroll

Lagring av trafikkdata kan reise spørsmål om hvilken grad av overvåkning man ønsker i et samfunn. Selv om formålet med lagringen er et annet, kan det argumenteres med at selve eksistensen av lagre med slikt omfang av personopplysninger strider mot interessen i forholdsmessig kontroll.

[32] Se nærmere om spørsmålet om uforenlighet under punkt 2.1.1

3.2 Behovet for effektive etterforskningsmetoder

3.2.1 Innledning

Hvilke etterforskningsmetoder det til enhver tid er behov for, er avhengig av kriminalitetstrusselen. Trusselnivået vil avhenge av flere forhold, bl a hvor mye kriminalitet som begås og utvikling i metoder som gjør at man forutser økning i begåtte lovbrudd. I det følgende redegjøres det først for kriminalitetsbilde og til sist nærmere om hvilke metoder politiet mener er påkrevd i denne sammenheng

3.2.2 Kriminalitetsbildet

Fortsatt blir det meste av kriminaliteten begått på tradisjonell måte, hvilket betyr at det skjer innenfor et avgrenset geografisk område, og uten noen form for organisering. Kriminaliteten i Norge er likevel nå på et nivå et nivå som fordrer helhetlig, tverrfaglig, grensesprengende innsats dersom politiet skal ha en reell sjanse til å bekjempe den. Utfordringene politiet står overfor er særlig kjennetegnet ved at de kriminelle aktørene viser økt grad av profesjonalisering og at organisasjonene ofte er internasjonale og multikriminelle[33].

.

I løpet av de siste årene har det skjedd en økning og endring i kriminalitetsbildet, internasjonalt som her til lands. Dette gjelder både kriminaliteten i seg selv, dvs hvilke type lovbrudd som blir begått er forandret, men også hvilke metoder de kriminelle benytter seg av. Det er flere utviklingstrekk i teknologien som gjør at metoder for å begå kriminalitet har endret seg. Den rivende utvikling av elektroniske kommunikasjonsmidler er også noe kriminelle vet å utnytte. Stor vekst i bruken av Internett og elektroniske tjenester, og utvikling i teknologien gir stadig flere muligheter for kriminell atferd, samtidig som den gjør at kriminaliteten ikke lenger kjenner territorielle grenser. Kommunikasjonsmidlene blir mer mobile, har større overføringskapasitet og er billige måter å kommunisere over landegrenser. De gjør det dessuten mulig å begå lovbrudd i ett land, mans man fysisk befinner seg i et annet.

---

[33] Kripos' årsrapport 2002.

Kriminalitet kan begås uten at gjerningsmannen og offeret noen gang har hatt kontakt med hverandre[34]. Oppdagelsesrisikoen synker når kriminaliteten krysser landegrensene.

Økt grad av organisering, internasjonalisering og mobilitet vanskeliggjør oppklaringen av lovbrudd. Problemer med organisert kriminalitet er at den gjør bruk av avansert teknologi, metoder og operasjonskonsepter med høy grad av profesjonalitet. Disse forhold gjør denne typen kriminalitet ekstra vanskelig å bekjempe. Et markant utviklingstrekk er at man ser en kobling mellom narkotikakriminalitet og annen kriminalitet; såkalt multikriminalitet. Dette gjør at f eks narkotikakriminalitet ikke kan ses som et isolert problem. Det er et grunnleggende samfunnsproblem som gir ringvirkninger på annen kriminalitet og samfunnsutviklingen generelt.

Et særtrekk ved nyere kriminalitet er at den er vanskelig å etterforske ved tradisjonelle etterforskningsmetoder. De nye kriminalitetsmetoder krever nye og mer effektive metoder for å forebygge, oppklare og avdekke kriminalitet. Slike midler kan være mulighet til å kartlegge bruken av elektronisk kommunikasjon. Tilgang til trafikkdata er ett virkemiddel her.

Elektroniske bevis spiller en stor rolle ved etterforskning av alle typer kriminalitet, ikke kun datakriminalitet. Det er brukt i mange typer straffesaker; utpresning, narkotikakriminalitet, drapssaker, økonomiske straffesaker og saker med seksuelle overgrep mot barn[35]. Før endringene i straffeprosessloven kap 16 a ble gitt, ble det satt ned et metodeutvalg som skulle vurdere kriminalitetsutviklingen og behovet for nye etterforskningsmetoder. Metodeutvalget konkluderte med at det har skjedd en økning i kriminaliteten og at kriminaliteten har endret karakter. Dette gjør at det foreligger et reelt behov for nye etterforskningsmetoder. Dette ble kritisert fra flere hold. Kritikken bestod i at grunnlaget for å konstatere økning i kriminalitetens omfang var utilstrekkelig. Økningen kunne forklares med andre forhold, bl a at rutinene for statistikk over begåtte lovbrudd var endret i den aktuelle perioden. Videre ble det

[34] Stortingsmelding nr 22 (2000-2001) s 18 og 19.

[35] Jf Sunde 2000

fremholdt at redegjørelsen av kriminalitetsbildet var for unyansert. Departementet fant at mesteparten av kritikken gikk på at man var uenig i hvordan økningen i kriminaliteten var målt, mens det knapt var noen innsigelser mht vurderingen av at kriminaliteten hadde endret karakter. Departementet fant at dette momentet alene gjorde nye ekstraordinære etterforskningsmetoder påkrevd.

De nye etterforskningsmetodene kan utfordre hensynene til personvern og rettssikkerhet. Politiet blir stadig oftere stilt overfor slike avveininger; valget mellom effektive etterforskningsmetoder og rettsikkerhet og personvern[36]. Bruk av metoder som sporer kartlegger bruk av elektronisk kommunikasjon, tilhører de ekstraordinære etterforskningsmetoder. Dette er metoder som er mer inngripende overfor den de rettes mot, og som det kreves mer for å ta i bruk. Bruk av slike metoder forutsetter at det foretas en forholdsmessighetsvurdering. Inngrepet overfor den mistenkte må klart veies opp av de fordeler metoden gir. Det må være "av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort", jf strpl § 216 c. Det sentrale er at politiet ikke kan benytte et ekstraordinært etterforskningsmiddel kun fordi saken vil bli oppklart raskere; det kreves noe mer.

Mer om de enkelte kriminalitetstyper og behov for etterforskningsmetode[37]
Ved "vanlig" vold vil de ordinære etterforskningsmetoder fortsatt være tilstrekkelig. Vold begås imidlertid i stadig større grad i forbindelse med annen kriminalitet; organisert kriminalitet, narkotikakriminalitet eller kriminalitet relatert til MC-miljøene. I disse tilfeller er voldsbruken ofte svært grov, og oppklaring av sakene er vanskelig fordi vitner ikke tør å samarbeide med politiet av frykt for represalier. Et annet særtrekk er tendensen til å oppklare forhold ved en form for indre justis. Dette gjør kriminalitetsbekjempelse i disse miljø vanskelig.

Når det gjelder narkotikamiljøene, er det fra politiets ståsted klart at de tradisjonelle etterforskningsmetoder ikke er tilstrekkelige. Kriminalitet i disse miljøene vil ofte ikke

---

[36] Stortingsmelding nr 22 (2000-20001) s 13.

[37] NOU 1997:15.

anmeldes, fordi offer og gjerningsperson har sammenfallende interesser. Bruk av kommunikasjonskontroll i etterforskning ble først iverksatt for disse sakene. Spritsmugling blir ofte begått av de samme personer som står for narkotikakriminaliteten. Det er derfor de samme hensynene som gjør seg gjeldende her. Ved etterforskning av datakriminalitet er bruk av trafikkdata påkrevd. Vinningsforbrytelser vil i stor grad la seg løse ved bruk av vanlige metoder, men det kan stille seg annerledes hvor slik kriminalitet inngår i annen kriminalitet, f eks narkotika. Når det gjelder sedelighetssaker, vil bruk av nye metoder som infiltrasjon være av stor betydning for muligheten til oppklaring av lovbrudd. Menneskesmugling er en forholdsvis ny type kriminalitet, som i stor grad følger samme mønster som utøvelse av narkotikakriminalitet. De samme hensyn gjør seg derfor gjeldende her. MC-miljøene preges av at de er svært lukket og vanskelig tilgjengelig for politiet. Kriminalitet begått her vil derfor vanskelig la seg oppklare ved hjelp av vanlige metoder. Nye metoder som f eks romavlytting er derfor ønskelig fra politiets side. Terrorrisikoen kan ikke sies å være stor i Norge. Kriminalitet av denne type kjennetegnes imidlertid av kommunikasjon; bruk av Internett er av stor betydning.

3.2.3 Ønsket regulering fra politiets ståsted[38]

Slik politiet ser det, er det nødvendig at opplysninger om abonnementsforhold og trafikkdata loggføres. Disse sporene kan være viktige både ved kriminalitet der selve lovbruddet begås ved hjelp av IKT, men også der spor fra bruk av elektronisk kommunikasjonsmiddel har betydning som bevis og for oppklaring av saken. Politiets erfaring viser at det er påkrevd at det foreligger logger som kan spore bruken av en kommunikasjonstjeneste til abonnent. Dette forutsetter at det ikke kan være adgang til å tilby anonyme kommunikasjonstjenester hvor brukeren ikke kan identifiseres for politiet. Loggene og abonnentsdataene må lagres i minst ett år etter at bruken skjedde. Det må videre være mulighet for å forlenge oppbevaringen i enkelttilfeller på politiets anmodning i forbindelse med etterforskning. Dessuten må opplysningene utleveres direkte til politiet i forbindelse med etterforskning. Videre må

[38] Sunde 2000

regelverket sikre at det stilles like krav til tilbydere av elektronisk kommunikasjon via offentlig nett, uavhengig av hvilken teknologi som er benyttet.

4 Rettstilstanden de lege lata

4.1 Innledning

I det følgende redegjøres det for gjeldende rett; norsk lovgivning og internasjonale rettskilder. EMK er inkorporert i norsk rett[39], men blir her behandlet under de internasjonale rettskilder, da konvensjonen er utarbeidet på internasjonal plan.

4.2 Norsk lovgivning

4.2.1 Personopplysningsloven

Lov av 14. april 2000 nr 31 om behandling av personopplysninger[40] (personopplysningsloven) regulerer behandling av personopplysninger, jf peol § 3. Loven gjennomfører direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

Hvorvidt loven kommer til anvendelse på lagring av trafikkdata, avhenger for det første av om trafikkdata dekkes av begrepet personopplysninger, og dernest om lagring av trafikkdata er en behandling i lovens forstand.

Begrepet personopplysning er definert som "opplysninger og vurderinger som kan knyttes til en enkeltperson" pol § 2, 1. Problemstillingen blir etter dette om trafikkdataene kan knyttes til en enkeltperson. Det sentrale her er muligheten for identifikasjon, ikke opplysningenes eller vurderingenes art. Både direkte og indirekte identifikasjon er omfattet[41]. Det kreves at en person må kunne knyttes til en opplysning med en forholdsvis stor grad av sikkerhet[42]. Hva som er tilstrekkelig identifikasjon, må vurderes for hvert enkelt tilfelle. I denne sammenheng oppstår det spørsmål om et telefonnummer kan identifisere en person. I utgangspunktet kan et telefonnummer indirekte identifisere en person, dersom den telefonnummeret er registrert på også er

---

[39] Jf punkt 2.2.2.

[40] Loven gjennomfører direktiv?

[41] Se NOU 1997:19 s 52

[42] Jf Bygrave og Schartum kapittel 4 s 13.

den som bruker telefonen. Dette vil i stor grad være tilfellet med mobiltelefoner; de fleste som har en mobil benytter den til personlig bruk, og det er stadig vanligere at "alle " har en egen mobiltelefon. Dersom den registrerte og bruker ikke er samme person, oppstår det spørsmål om kravet til identifikasjon er oppfylt. Dette gjelder f eks når telefonabonnementet er registrert på en person, mens det er flere brukere, som tilfellet ofte er i en familie. Her vil hensynet til beskyttelse av personvernet i formålsbestemmelsen i § 1 kunne komme inn som et tolkingsmoment[43], slik at trafikkdata i slike tilfeller vil regnes som personopplysninger.[44] Også i tilfeller der flere personer benytter samme IP-adresse, oppstår spørsmålet om hvor liten gruppen av brukere må være for at kravet til identifikasjon er oppfylt[45].

Den neste problemstillingen er så om lagring av slike data er en behandling av personopplysninger. Loven gjelder for all behandling som helt eller delvis skjer med elektroniske hjelpemidler, jf § 3 a). Behandling er i § 2 nr 2 definert som "enhver bruk av personopplysninger, som f eks innsamling, registrering, sammenstilling, *lagring* og utlevering eller en kombinasjon av slike bruksmåter". Lagring av trafikkdata omfattes dermed av ordlyden.

Det er etter dette klart at lagring av trafikkdata er en behandling av personopplysninger som reguleres av pol. Det neste tema er derfor hvilke krav pol stiller til behandling av personopplysninger. Det er først nødvendig å si noe om *hvem* kravene retter seg mot. Subjektet for kravene er den behandlingsansvarlige, jf pol § 11. Med dette menes den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf pol § 2, punkt 4. I denne sammenhengen vil tilbyder av teletjenester[46] være behandlingsansvarlig.

---

[43] Jf Ot prp nr 92 (1998-99) s 101.

[44] Se Bygrave og Schartum kapittel 4 s 13

[45] Jf Bygrave 2002 s 318.

[46] Teletjeneste: tilbud i næringsøyemed om formidling av telekommunikasjon helt eller delvis ved hjelp av overføring i telenett, som ikke er kringkastning, jf teleloven § 1-6 bokstav d. F eks Telenor og NetCom.

Grunnkravene til behandling av personopplysninger følger av pol § 11. Etter denne må for det første vilkårene for behandling som stilles i §§ 8 og 9 være oppfylt. Det er § 8 som kommer til anvendelse her, da § 9 gjelder for sensitive personopplysninger[47]. Etter § 8 kan behandling av personopplysninger bare skje dersom det foreligger samtykke fra den registrerte[48], hvis adgang til behandlingen er fastsatt i lov, eller dersom behandlingen er nødvendig for ett eller flere nærmere angitte formål.

For at et samtykke skal godtas som grunnlag for behandling av personopplysninger, kreves det at samtykket er frivillig, informert og uttrykkelig, jf pol § 2 nr 7. Det følger av forarbeidene at behandling av personopplysninger i størst mulig grad bør baseres på samtykke fra den registrerte[49]. Det er i dette tilfellet ikke samtykke som er grunnlag for tilbydere av teletjenester sin behandling av trafikkdata. Det kan i medhold av teleloven gis forskrift om lagring av opplysninger. Denne hjemmelen er ikke benyttet, det er følgelig ikke fastsatt i lov at tilbydere av teletjenester skal lagre trafikkdata. Behandlingen må derfor være nødvendig for ett eller flere av følgende formål:

a) å oppfylle en avtale med den registrerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås,
b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse,
c) å vareta den registrertes vitale interesser,
d) å utføre en oppgave av allmenn interesse,
e) å utøve en offentlig myndighet, eller
f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen.

Betaling av teletjenester er en del av oppfyllelsen av en avtale om levering av teletjenester. Spørsmålet blir så om lagring av trafikkdata er nødvendig for å kunne

---

[47] opplysninger om a)rasemessig eller etnisk bakgrunn, eller politisk, filosofisk, eller religiøs oppfatning, b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, c) helseforhold, d)seksuelle forhold, e) medlemskap i fagforeninger , jf § 2, pkt 8.

[48] Registrert: den som en personopplysning kan knyttes til, jf pol § 2 nr 6.

[49] Ot prp nr 92 (1998-99) s 108.

fakturere for bruken av tjenesten. Lagringen kan ikke anses som et gjøremål etter den registrertes ønske før avtalen inngås. Heller ikke alternativ b kommer til anvendelse her. Alternativ c om vitale interesser er gitt for de tilfeller hvor behandling av opplysninger er av vesentlig betydning for den registrertes liv[50], og er heller aktuelt i denne sammenheng. Det kan også vanskelig argumenteres med at lagring av trafikkdata er en oppgave av allmenn interesse, eller utøvelse av offentlig myndighet, så alternativene d og e er også utelukket her.

Det siste mulige alternativet er etter dette bokstav f. Problemstillingen her hvorvidt tilbyderne av teletjenester eller tredjepersoner som trafikkdataene utleveres til ivaretar en berettiget interesse som ikke overstiges av hensynet til den registrertes personvern. Dette er en slags samlebestemmelse som brukes når man ikke finner grunnlag i de øvrige alternativene. Det oppstilles her krav til interesseovervekt[51]. Vurderingen skal foretas av den behandlingsansvarlige[52], men Datatilsynet har et ansvar for å gi råd og veiledning om denne interesseavveiningen, jf pol § 42 tredje ledd nr 6. Datatilsynet kan dessuten overprøve dette skjønnet, jf pol § 46. Det fremheves i forarbeidene at interessen til den registrertes personvern må tillegges betydelig vekt i avveining mot kommersielle interesser. Det ble foretatt en avveining (etter personregisterloven) mellom behovet for lagring av trafikkdata og hensynet til den registrertes personvern da Televerket (nå Telenor) søkte konsesjon for å innføre et sentralisert takseringssystem (Sentaks)[53]. Justisdepartementet fant da at de personvernmessige problemene ikke var av en slik art at systemet ikke burde bli innført[54]. Det må være dette som er hjemmelen for at tilbyderen av teletjenester kan behandle personopplysninger. Den behandlingsansvarlige kan på visse vilkår bli erstatningspliktig dersom behandlingen har skjedd på et utilstrekkelig grunnlag, jf pol § 49.

---

[51] Bygrave og Schartum kapittel 4 s 29.

[52] Jf Wiik Johannesen s 103.

[53] Se Ingvild Hanssen Bauer: Personvern i digitale telenett (Complex 3/93) for en nærmere redegjørelse av dette.

[54] Se Bygrave 1997 s 136 flg.

Pol § 11 stiller i tillegg til vilkårene behandlet ovenfor visse krav om behandlingens formål, jf bokstav b og c. Etter bokstav b kan personopplysningene bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet. Dette kravet innebærer at den behandlingsansvarlige skal fastsette formål før behandlingen tar til, som er tilstrekkelig konkret, presist og avgrenset til at det er klart og åpent hva behandlingen skal tjene til[55].
Dersom de innsamlede opplysningene skal brukes til nye formål som ikke er dekket av den opprinnelige formålsangivelsen, må det nye formålet oppfylle kravene til lovlig behandling i § 8. I tillegg stiller bokstav c krav om at personopplysningene ikke brukes til senere formål som er uforenlige med det opprinnelige formålet med innsamlingen, uten at den registrerte samtykker. Dette et uttrykk for prinsippet om formålsbestemthet, jf ovenfor under avsnitt 3.1.4. Hvorvidt det nye formålet er uforenlig med det opprinnelige, beror på en konkret og individuell vurdering. Hvorvidt bruken av opplysningene innebærer en ulempe for den registrerte, og om bruken skiller seg sterkt fra den opprinnelige, vil være sentrale momenter ved denne vurderingen[56]. Dersom det legges til grunn at kravet om "ikke-uforenlighet" er et uttrykk for at det skal tas hensyn til hva den registrerte med rimelighet kan forvente at opplysningene blir brukt til, må det kreves at det nye formålet må ligge innenfor hva den registrerte kan lese ut av det opprinnelige formålet[57]. Det opprinnelige formålet med lagringen av trafikkdataene er fakturering og gjennomføring av tjenesten, jf nedenfor. Når politiet innhenter trafikkdataene, er formålet kriminalitetsbekjempelse. Disse formålene kan vanskelig sies å være forenlige. Politiets tilgang er imidlertid hjemlet i lov, og er derfor ikke i strid med legalitetsprinsippet.

De øvrige grunnkravene til behandling av personopplysninger er at opplysningene skal være tilstrekkelige og relevante i forhold til formålet med behandlingen (bokstav d), og at opplysningene er korrekte og oppdaterte, og ikke lagres lenge enn det som er nødvendig ut fra formåler med behandlingen.

---

[55] Ot prp nr 92 (1998-99) s 114.

[56] Ot prp nr 92 (1998-99) s 113.

[57] Jf Bygrave 2002 s 340.

Øvrige krav som stilles i pol:
Pol § 13 stiller krav om informasjonssikkerhet. Kravene retter seg mot den behandlingsansvarlige og databehandleren[58], som gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Dette forutsetter at det etablering av både organisatoriske og tekniske sikkerhetstiltak[59]. Det er særlig kravet til konfidensialitet som er av interesse her. Dette kravet skal sikre at informasjon ikke skal gjøres tilgjengelig for uvedkommende under behandlingen, f eks ved bruk, transport og lagring. Etter § 13, annet ledd skal informasjonssystemet og sikkerhetstiltakene dokumenteres.

Den behandlingsansvarlige pålegges videre i pol § 14 å etablere og holde ved like planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder å sikre personopplysningenes kvalitet. Med kvalitet menes her korrekte, fullstendige og aktuelle opplysninger som er relevante for formålet med behandlingen[60].

Behandling av personopplysninger krever i utgangspunktet ikke konsesjon fra Datatilsynet[61], med mindre det dreier seg om sensitive personopplysninger, jf § 33. Trafikkdata er ikke sensitive personopplysninger[62]. Tilbydere av teletjenester er i personopplysningsforskriften § 7-1, jf pol § 31 fjerde ledd, ilagt konsesjonsplikt for behandling av personopplysninger for kundeadministrasjon, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av telenett. Datatilsynet har gitt flere tilbydere av teletjenester konsesjon til å behandle personopplysninger[63]. Opplysninger om teletrafikken lagres for å gi grunnlag for faktureringen og en eventuell klagebehandling.

---

[58] Den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf pol § 2 nr 5.

[59] Ot prp nr 92 (1998-99) s 114.

[60] Ot prp nr 92 (1998-99) s 116.

[61] Jf pol § 33. Se pol § 42 om Datatilsynets organisering oppgaver.

[62] Jf note nr 15.

[63] Fremstillingen her er basert på konsesjon gitt til Telenor, men dette er en standardkonsesjon, slik at det i hovedsak vil være de samme vilkårene som gjelder for alle tilbydere av teletjenester.

Om de øvrige vilkårene i konsesjonen:
Det stilles som vilkår at formålet med behandlingen av opplysningene er kundeadministrasjon, opplysningstjenestes, fakturering og gjennomføring av tjenester i forbindelse med abonnentens bruk av telenett, inklusive samtrafikkavregning[64]. Hvis opplysningene skal brukes til andre formål, må den behandlingsansvarlige sørge for at dette skjer i henhold til personopplysningsloven. Konsesjonen setter videre som vilkår at det bare behandles opplysninger som er nødvendige for gjennomføring og fakturering av tjenesten (konsesjonens punkt 2). I konsesjonens punkt 8 oppstilles det en sletteplikt for opplysningene. Personopplysninger som benyttes til faktureringsformål skal slettes når fakturaen er gjort opp, eventuelt når klagefristen er gått ut. Dette er i tråd med grunnkravet i pol § 11, bokstav e. For tjenester med månedlig fakturering skal opplysningene slettes senest tre måneder etter at de ble registrert, og for tjenester med kvartalsvis fakturering skal sletting skje senest etter fem måneder. Dersom en faktura ikke blir betalt eller det oppstår en rettslig tvist, kan opplysningene lagres til kravet er gjort opp eller rettslig avgjort. Opplysninger som er nødvendige for oppkobling og gjennomføring av tjenesten, skal slettes så snart tjenesten er nedkoblet.

Konsesjonen angir ikke konkret hvilke opplysninger som kan behandles. Dette skal avgjøres konkret i hvert tilfelle.

Det er etter konsesjonens punkt 6 i utgangspunktet ikke adgang til å utlevere personopplysninger til utenforstående. Slik utlevering kan unntaksvis skje når den opplysningen gjelder har samtykket[65] til det, hvis det skjer med hjemmel i lov (eller i forskrift gitt med hjemmel i lov), som ledd i betalingsinnkreving eller som ledd i regnskapsbehandling.

[64] Hva er dette? Se konsesjonen

[65] Det kreves her et frivillig, uttrykkelig og informert samtykke, jf konsesjonens punk 6 nr 1.

4.2.2 Teleloven

Lov av 23. Juni nr 39 1995 om telekommunikasjon omfatter all telekommunikasjonsvirksomhet. Med telekommunikasjonsvirksomhet forstås overføring av lyd, tekst, bilder eller andre data ved hjelp av lys, radiosignaler eller andre elektromagnetiske signaler i et kommunikasjonssystem for signalbefordring, jf § 1-6 litra a. Det sentrale vilkår for at en virksomhet skal dekkes av loven, er altså at det foregår en overføring av elektromagnetiske signaler. Både telefoni og bruk av Internett omfattes av dette begrepet.

Den første problemstillingen er hvorvidt det oppstilles en lagringsplikt for trafikkdata etter teleloven. Telel § 3-4 gir hjemmel for å stille krav til tilbyder om lagring og utlevering av opplysninger. Denne hjemmelen ikke fulgt opp i forskriften når det gjelder lagring av opplysninger. Det er heller ikke stilt krav om slik lagring som et vilkår i konsesjon eller ved pålegg[66]. Tilbyderne har med andre ord ingen generell *plikt* til å lagre opplysninger om sluttbrukernes bruk av tjenesten. Hva som rent faktisk blir lagret, følger av konsesjonen, jf punkt 4.2.1.

Tilgang til trafikkdata etter telel

Når det gjelder utlevering av opplysninger, er dette nærmere regulert av § 9-3[67]. Denne forutsetter at visse opplysninger blir lagret. Utgangspunktet etter denne er at tilbyder har taushetsplikt når det gjelder innholdet av telekommunikasjon og andres bruk av telekommunikasjon, jf første ledd. Taushetsplikten omfatter ikke egen bruk av telekommunikasjon, slik at den som tar del i telekommunikasjon fritt kan motta opplysninger om trafikk til og fra seg selv, jf "andre enn de som opplysningene gjelder", jf § 9-3 første ledd annet punktum.

Regelen gir ingen nærmere beskrivelse av hva som omfattes av begrepet "innhold". Det som etter denne bestemmelsen er underlagt taushetsplikt, er de ulike typene data som er

---

[66] Jf Sunde 2000

[67] Telel § 7-7 understøtter taushetsplikten i § 9-3, ved at den gir hjemmel for å gi pålegg om at det i telenett og ved tilbud om teletjeneste skal gjennomføres sikringstiltak av hensyn til rikets sikkerhet, personvernet, taushetsplikt eller andre viktige samfunnsinteresser(…)

generert ved kommunikasjon fra abonnent eller andre i telenettet, uavhengig av hvilken tjeneste det dreier seg om, f eks telefoni i fastnett eller mobilnett, datakommunikasjon osv. Først og fremst vil taushetsplikten omfatte, foruten identifikasjon av tjeneste, hvem som har kommunisert, til hvilket tidspunkt og varigheten av forbindelsen[68]. Brudd på denne bestemmelsen begått av noen som regelen retter seg mot, vil kunne rammes av straffeloven § 121.

Tredje ledd i § 9-3 oppstiller visse unntak fra hovedregelen om taushetsplikt. Etter denne kan det gis opplysninger om registrert navn, adresse, telefonnummer eller datakommunikasjonsadresse til påtalemyndighetene eller politiet. Det samme gjelder ved vitnemål for retten. I fjerde ledd befestes unntaket i tredje ledd ved å fastslå at anmodninger om de opplysninger som er unntatt fra taushetsplikten skal "etterkommes med mindre særlige forhold gjør det utilrådelig." Abonnentsdata er med andre ord ikke taushetsbelagt, mens trafikkdata er det. Det blir derfor nødvendig å klarlegge innholdet av unntaket fra taushetsplikten.
Det var tidligere en viss tvil om omfanget av unntaket fra taushetsplikten, men dette er nå klargjort ved en avgjørelse fra Høyesterett. I Rt 1999 s 1944 kom Høyesterett under dissens frem til at også dynamiske IP-adresser er omfattet av begrepet "datakommunikasjonsadresse".

Det er også andre unntak fra hovedregelen om taushetsplikt for innholdet av telekommunikasjon. For det første er ikke taushetsplikten til hinder for at den som er part i telekommunikasjon selv kan innhente opplysninger om sin egen trafikk, eller mer vesentlig her; gi sitt samtykke til at politiet får disse opplysningene. Også nødrettsbetraktninger kan føre til at det gis unntak fra taushetsplikten. Dette kan være aktuelt i forbindelse med forsvinningssaker eller redningsaksjoner. Jeg vil ikke gå nærmere inn på disse problemstillingene. Det er videre flere regler i straffeprosessloven som kan gi unntak fra taushetsplikten, bl a reglene om vitneplikt, utleveringspålegg, kommunikasjonskontroll. Dette vil bli behandlet nedenfor i punkt 4.2.4.

[68] Bing m fl s 274

4.2.3 Forslag til ny lov om elektronisk kommunikasjon (ekomloven)

I ot prp nr 58 (2002-2003) foreslås ny lov om elektronisk kommunikasjon (ekomloven), som skal erstatte dagens telelov. Lovforslaget tar hensyn til at tele-, media/kringkastning- og IT-sektorene har smeltet sammen (konvergert), og utvider virkeområdet i forhold til gjeldende telelov til å omfatte all virksomhet innenfor området for elektronisk kommunikasjon. Lovforslaget legger til rette for harmonisering med EU-lovgivningen gjennom lov og forskrifter, samt ved den løpende forvaltningen av regelverket[69]. Relevant i denne sammenhengen er direktiv 02/58. Det tas sikte på at loven skal tre i kraft 25. juli 2003, samtidig med at det nye regleverket trer i kraft i EU.

Forslagets §§ 2-7 og 2-8 gir regler om behandling av trafikkdata. Det første spørsmålet er her som ovenfor; hva sier lovforslaget om oppbevaring av trafikkdata.
Dette reguleres av lovforslagets § 2-7. Denne pålegger tilbyder å gjennomføre nødvendige sikkerhetstiltak til vern av kommunikasjon i egne elektroniske kommunikasjonsnett- og tjenester, jf første ledd. I annet ledd pålegges tilbyderne plikt til å slette eller anonymisere trafikkdata så snart de ikke lenger er nødvendig for kommunikasjons- eller faktureringsformål. Dette følger i dag av standardkonsesjonen som gis av Datatilsynet i medhold av personopplysningsforskriften § 7-1. Forslagets § 2-7 if åpner imidlertid for at annet kan følge av lov eller i medhold av lov.

Politiet og påtalemyndighetene er avhengig av at trafikkdataene er av en viss kvalitet for at de skal kunne dra nytte av disse opplysningene der de har lovbestemt hjemmel til det (f eks etter strpl kap 16 a). Lovforslagets § 2-8, første ledd pålegger tilbyderne en tilretteleggingsplikt for påtalemyndighetene og politiet for lovbestemt tilgang til informasjon. Dette er i dag regulert i offentlignettforskriften § 2-11, jf telel § 3-4, 1. ledd bokstav h.

Det åpnes ikke for å pålegge permanent lagringsplikt for trafikkdata i dette lovforslaget, men § 2-8 annet ledd gir hjemmel for myndighetene til å gi forskrifter om denne tilretteleggingsplikten, herunder om plikt til å lagre trafikkdata i en bestemt periode.

---

[69] Avskrift fra otprp s 2 (under innledning og sammendrag)

Departementet avventer Datakrimutvalgets[70] innstilling før lagringsplikt eventuelt blir permanent. Inntil da åpnes det for at lagringsplikt kan pålegges midlertidig i forskrift gitt med hjemmel i § 2-8, annet ledd. Dette kan være aktuelt f eks dersom det viser seg at det blir vanlig at tilbyder sletter eller anonymiserer informasjon om sluttbruker og elektronisk kommunikasjon før plikten etter § 2-7 til å gjøre det inntrer, og dette fører til at de lovbestemte tilgangene til informasjon(f eks reglene om kommunikasjonskontroll) ikke kan oppfylles. Det presiseres at Stortinget skal involveres før det evt skal fastsette lagringsplikt i forskrift.

Telelovens regler om taushetsplikt videreføres så å si uendret i forslagets § 2-9. Denne Endringer her består hovedsakelig i at begrepet "telekommunikasjon" er erstattet med det mer teknologinøytrale "elektronisk kommunikasjon". Videre er det i bestemmelsens tredje ledd særskilt angitt at også opplysninger om elektronisk kommunikasjonsadresse omfattes. Dette skal sees på bakgrunn av Høyesteretts dom i Rt 1999 s 1944[71]. Det er videre presisert at taushetsplikten i første ledd ikke er til hinder for at opplysninger som nevnt i første ledd gis til annen myndighet i medhold av lov. Dette er gjort for å klargjøre at det ikke er motstrid mellom lovene der annen lov gir rett til innsyn i lovens taushetsbelagte opplysninger.[72]

4.2.4 Straffeprosessloven[73]

4.2.4.1 Vitneplikt

Unntak fra taushetsplikten etter telel § 9-3, 1.ledd kan følge av regler om vitneplikt for retten og forklaringsplikt for politiet i strpl. Etter strpl § 108 er hovedreglen et alminnelig prinsipp om vitneplikt. Regelen slår fast at "enhver plikter etter innkalling å møte som vitne og forklare seg overfor retten(…)". Det følger av dette at tilbydere av teletjenester har vitneplikt overfor retten. § 118 gir imidlertid unntak fra dette for "(…)forklaring som vitnet ikke kan gi uten å krenke lovbestemt taushetsplikt han har

---

[70] Utvalg nedsatt for å vurdere bl a forholdet til konvensjonen om cybercrimemandat..

[71] Jf Ot prp nr 58 (2002-2003). Se også redegjørelsen for denne dommen i punkt 4.2.2 ovenfor.

[72] Ot prp nr 58 (2002-2003)

[73] Heretter strpl.

som følge av tjeneste eller arbeid for stat eller kommune, familievernkontor, postoperatør eller tilbyder av tilgang til telenett eller teletjeneste eller teleinstallatør, hvis ikke departementet gir samtykke(…)", jf strpl § 118, 1.ledd, 1.pkt. Departementets myndighet er delegert til Post- og teletilsynet (PT) ved brev av 14. desember 1995.

§ 118 gir PT adgang til å gi samtykke om fritak fra taushetsplikten, men angir også retningslinjer for PT sin avgjørelse. PT kan bare nekte samtykke dersom åpenbaringen vil kunne utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighold, jf § 118 første ledd annet punktum. Sistnevnte vil typisk være hensynet til personvern for den berørte.
Dessuten kan retten ved kjennelse, etter en avveining av hensynet til taushetsplikten og hensynet til sakens opplysning, bestemme at vitneforklaring skal gis selv om samtykke er nektet, eller motsatt; at vitneforklaring ikke skal mottas selv om PT har samtykket, jf § 118, annet ledd.

Hvilken praksis har så PT lagt seg på ved vurderingen av om samtykke til fritak fra taushetsplikt skal gis?[74] Vurderingstemaet er som vist ovenfor angitt i § 118; det beror på en avveining mellom etterforskningshensyn (jf "utsette staten eller allmenne interesser for skade") og personvernhensyn (jf " virke urimelig overfor den som har krav på hemmelighold"). Post- og teletilsynet sin oppgave er her å "vurdere(r) styrken på mistanken, hvilken bevisverdi opplysninger om telekommunikasjon vil ha for saken, hvorvidt det finnes mindre inngripende tiltak som politiet bør prøve først, dessuten hvor sterk / sannsynlig forbindelsen mellom et gitt abonnement og en konkret siktet / mistenkt person er." Graden av mistanke vil ofte være prøvet av domstolene før Post- og teletilsynet blir bedt om å gi fritak fra taushetsplikten, dersom siktede er varetektsfengslet. Post- og teletilsynet vil da i utgangspunktet gi samtykke til utlevering av opplysningene, dersom dette er relevant for saken. Videre må perioden politiet anmoder om trafikkdata for være knyttet til gjerningstidspunktet

[74] Fremstillingen er her basert på Fuhr m fl.

4.2.4.2 Forklaringsplikt for politiet

Politiet kan med hjemmel i strpl § 230 la oppta forklaring fra mistenkte, vitner og sakkyndige, men disse er ikke underlagt noe forklaringsplikt overfor politiet på etterforskningsstadiet. Regelen retter seg mot mistenkte, vitner og sakkyndige.
§ 230, annet ledd henviser til § 118 første og annet ledd, slik at dersom tilbyder er omfattet av denne regelen, gjelder samme regler mht taushetsbelagte opplysninger som redegjort for ovenfor for vitneplikt for retten. Utgangspunktet er at tilbyder ikke kan forklare seg om innholdet av telekommunikasjon, siden dette er taushetsbelagt etter telel § 9-3, men at Post- og teletilsynet kan gi samtykke til å forklare seg om disse forhold. Det vil uansett ikke oppstå en forklaringsplikt på dette stadiet.

4.2.4.3 Kommunikasjonskontroll

Retten kan også gi politiet tilgang til trafikkdata med hjemmel i reglene om kommunikasjonskontroll i strpl § 216 b. Etter denne kan retten ved kjennelse gi politiet tillatelse til å foreta annen kontroll av kommunikasjonsanlegg (dvs annen enn kommunikasjonsavlytting, jf § 216 a). Slik kontroll kan bl a gå ut på
at eier eller tilbyder av nett eller tjeneste som benyttes ved kommunikasjon, skal gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse med anlegg (dvs telefoner, datamaskiner eller andre kommunikasjonsanlegg som den mistenkte besitter eller kan antas å ville bruke, jf § 216 b, annet ledd litra a), og andre data knyttet til kommunikasjon. For at retten kan treffe slik kjennelse, må ulike vilkår være oppfylt. Adgangen til opplysninger etter denne bestemmelse er knyttet til en bestemt person. Vilkårene for utlevering av trafikkdata etter denne bestemmelsen er at det foreligger skjellig grunn til mistanke om en handling eller et forsøk på handling som etter loven kan medføre straff av fengsel i fem år eller mer, eller rammes av straffeloven kapittel 8 (forbrytelser mot Statens selvstendighet og sikkerhet) eller 9 (forbrytelser mot Norges statsforfatning og statsoverhode), eller av §§ 145 annet ledd (beskyttelsesbrudd), 162 (narkotika), 204 første ledd bokstav d (barnepornografi), 317 (informasjonsheleri), jf §§ 162 eller 390 a (krenker en annens fred).

Ved vurdering av om vilkåret om fare for fem års fengsel er oppfylt, skal ikke forhøyelse av maksimumsstraffen ved gjentakelse eller sammenstøt av forbrytelse tas i betraktning, jf §216 b, annet ledd, jf 216 a, annet ledd.

Det kan kun gis tillatelse til kommunikasjonskontroll dersom det må antas at slik kontroll vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort, jf § 216 c, første ledd. I saker som kan oppklares ved hjelp av ordinære etterforskningsmidler er politiet altså henvist til å benytte disse, selv om det ved kommunikasjonskontroll kunne ha oppklart saken raskere. Reglene om kommunikasjonskontroll er plassert i straffeprosesslovens tredje del om tvangsmidler, og bruk av kommunikasjonskontroll kan derfor ikke benyttes hvis ikke forholdsmessighetsprinsippet i strpl § 170 a er oppfylt. Det skal oppnevnes forsvarer for den mistenkte som blir utsatt for kommunikasjonskontroll, jf strpl § 100a.

Etter det Post- og teletilsynet kjenner til, blir strpl § 216 b annet ledd bokstav c normalt bare benyttet til å pålegge utlevering av trafikkdata ved samtidig beslutning om avlytting.[75]

4.2.4.4 Beslag og utleveringspålegg

Politiet har en alternativ tilgang til trafikkdata i de generelle reglene i strpl kapittel 16 om beslag og utlevering av ting som antas å ha betydning som bevis. Det følger av rettspraksis at begrepet ”ting” ikke bare omfatter fysiske gjenstander, men også opplysninger som lagres på data, og som kan gjøres tilgjengelige ved utskrifter, jf Rt 1992 s 905. Dette er også fulgt opp i flere senere avgjørelser[76]. I Rt 1998 s 309 slås det fast at ”ting” i strpl § 210, jf § 205 omfatter samtaledata, og at de vanlige reglene om beslag kan brukes parallelt med bestemmelsen i § 216 b. Det følger også av rettspraksis at pålegg om utlevering av registreringer av samtaler over en mobiltelefon kan gis med hensyn til fremtidige registreringer for et visst tidsrom, jf Rt 1997 s 470.

---

[75] Fuhr, Ringdal og Mørkved: Loven krever fritak fra taushetsplikten. (artikkel i Juristkontakt nr 2 2003)

4.3 Internasjonale rettskilder

4.3.1 EU: Direktiv 02/58/EF

Direktiv 2002/58/EF om behandling av personopplysninger og beskyttelse av privatlivets fred i den elektroniske kommunikasjonssektor erstatter og opphever gjeldende direktiv 97/66/EF om behandling av personopplysninger og beskyttelse av privatlivets fred innenfor telesektoren, jf artikkel 19. Fristen for implementering av det nye direktivet er satt til 31.oktober 2003, jf art 17. Direktiv 97/66/EF oppheves med virkning fra samme dato, jf art 19. Det er dette direktivet som skal implementeres ved ny lov om elektronisk kommunikasjon. Det spesifiserer og supplerer direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger. Direktiv 95/46 kommer til anvendelse på alle forhold vedrørende beskyttelse av grunnleggende rettigheter og frihetsrettigheter, som ikke er særlig omfattet av bestemmelsene i dette nye direktivet, jf fortalens punkt 10. Direktivene har samme anvendelsesområde; det gjelder ikke forhold som ikke er omfattet av fellesskapsretten, jf artikkel 1 nr 3 og fortalens punkt 11. Viktige områder som offentlig trygghet, forsvaret, statens sikkerhet og statens aktiviteter på det strafferettslige området faller derfor utenfor direktivets anvendelsesområde.

Det nye direktivet har til formål å tilpasse de eksisterende regler til teknologinøytrale alternativer. Det har videre som formål å styrke harmoniseringen innad i EU og EØS på den elektroniske kommunikasjonssektor når det gjelder beskyttelse av personopplysninger, privatlivets fred og juridiske personers legitime interesser, jf fortalens punkt 8.

Trafikkdata er i artikkel 2 b) definert som data som behandles for å overføre kommunikasjon i et elektronisk kommunikasjonsnett eller til fakturering av dette. Spørsmålene om lagring av trafikkdata reguleres av art 5, 6,og 15.

Artikkel 5 oppstiller et prinsipp om kommunikasjonshemmelighet. Denne pålegger medlemsstatene å sikre kommunikasjonshemmelighet ved bruk av offentlige kommunikasjonsnett og offentlig tigjengelig elektroniske kommunikasjonstjenester. Plikten omfatter både selve kommunikasjonen og de trafikkdata den genererer. Statene

skal etter denne bestemmelsen særlig forby avlytting, registrering, lagring og andre måter samtaler kan oppfanges eller overvåkes av andre enn brukerne, uten brukernes samtykke. Teknisk lagring som er nødvendig for overføring av kommunikasjon er likevel tillatt. Det er etter denne bestemmelsen i utgangspunktet forbudt å lagre trafikkdata.

Artikkel 6 regulerer trafikkdata spesielt. Utgangspunktet her er at trafikkdata som gjelder abonnenter og brukere skal slettes eller gjøres anonyme, når de ikke lengre er nødvendige for gjennomføring av kommunikasjonen, jf 1. ledd. Det er likevel tillatt å behandle trafikkdata for faktureringsformål og avregning for samtrafikk. Slik behandling er tillatt inntil utløpet av tidsrommet da regningen kan bestrides i medhold av lov eller betalingsinnkreving kan foretas[77], jf nr 2. ledd.

Artikkel 15 gir hjemmel for å gjøre unntak fra reglene omhandlet ovenfor. Etter denne kan medlemsstatene vedta lovforskrifter med formål å innskrenke rekkevidden av de rettigheter og forpliktelser som omhandles i artiklene 5,6,8 og 9. Forutsetningen for at dette kan skje, er at innskrenkningen er nødvendig, hensiktsmessig og forholdsmessig i et demokratisk samfunn av nærmere angitte hensyn, blant annet hensynet til den nasjonale sikkerhet, forsvaret, den offentlige sikkerhet, eller forebyggelse, etterforskning, avsløring og rettsforfølgelse av straffesaker eller til uautorisert bruk av elektroniske kommunikasjonssystem etter artikkel 13 i 95/46/EF. Medlemsstatene kan for disse hensyn vedta rettsregler om lagring av data i en begrenset periode.

Adgangen til å vedta denne type regler følger også av at direktivet ikke får anvendelse på de områder som nevnt ovenfor. Det slås imidlertid fast at direktivet ikke endrer den nåværende balanse mellom enkeltpersoners rett til privatlivets fred og medlemsstatenes mulighet til å treffe de tiltak som er nødvendige til vern av den offentlige sikkerhet, forsvaret, statens sikkerhet og statens aktiviteter på strafferettens område, jf fortalens punkt 11. Slike tiltak skal være hensiktsmessige, stå i åpenbart rimelig forhold til de mål, som forfølges, og tiltakene bør omfattes av hensiktsmessige beskyttelsesordninger i overensstemmelse med EMK.

---

[77] Definisjonen svarer til Sundes oversettelse av tilsvarende bestemmelse i 97/66/EF

4.3.2 Forslag til rammeavgjørelse

Det arbeides for tiden med en rammeavgjørelse innad i EU som skal regulere de viktige områder som er utelatt i direktiv 02/58/EF. Her foreslås det å pålegge lagringsplikt for trafikkdata det formål at politi og påtalemyndigheter får tilgang til det i sitt arbeid[78]. Spørsmål som det arbeides med her, er hvorvidt lagring av data kun kan skje for et konkret tilfelle, hvorvidt innholdsdata er omfattet, om det skal kreves rettslig kjennelse for tilgang til dataene og om det skal stilles faste vilkår[79]. Det er foreslått innføring av lagringsplikt på minst 12 måneder og maksimum 24 måneder[80]. En slik rammeavgjørelse vil være et vedtak som er bindende for de som avgjørelsen er rettet mot, jf Romatraktatens art 249.

4.3.3 Europarådets konvensjon om cybercrime

Hovedformålet med konvensjonen er å bekjempe ulike former for datakriminalitet, herunder pålegger den statene å kriminalisere barnepornografi som produseres eller distribueres via datasystem. Den inneholder imidlertid også prosessuelle bestemmelser som har virkning ved bekjempelse ved enhver form for kriminalitet, og det er disse som er relevante i denne sammenheng. (Konvensjonen til rette for internasjonalt samarbeide for å bekjempe cybercrime.) Den trer i kraft når minst fem stater, hvorav minst tre medlemsland, har ratifisert den, jf art 36. Per 06.04.03 har kun Albania og Kroatia ratifisert. Norge har kun undertegnet konvensjonen.

De prosessuelle reglene

Konvensjonen stiller visse minimumskrav til statenes prosessuelle lovgivning. Av disse er artikkel 14 den sentrale. Denne pålegger statene å implementere straffeprosessuelle regler som åpner for å utnytte elektronisk informasjon som bevis ved en straffbar handling, jf art 14,2, litra c. Konvensjonen gjelder dermed generelt på

---

[80] Jf artikkel i Statewatch

kriminalitetsbekjempelsens område, og omfatter alle straffesaker hvor dataetterforskning er relevant[81].

Den relevante bestemmelsen for lagring av trafikkdata er art 16. Denne pålegger statene å vedta de lover og andre virkemidler som er nødvendige for at de kompetente myndigheter hurtig skal kunne kreve bevaring av spesifiserte opplysninger, herunder trafikkdata, som har vært lagret i et datasystem. Dette gjelder særlig når det er grunn til å tro at dataene er spesielt sårbare for tap eller endring, jf art 16, 1. ledd.

Trafikkdata defineres her som data som knytter seg til kommunikasjon ved hjelp av et datasystem, generert av et datasystem som utgjorde en part i kjeden av kommunikasjon, og som angir kommunikasjonens opprinnelse, endested, rute, tidspunkt, dato, størrelse, varighet, eller type av underliggende service.

Art 16, 2 pålegger statene å innføre et system hvor den som besitter dataene kan pålegges å oppbevare disse så lenge som nødvendig, i inntil nitti dager, til de kompetente myndighetene får mulighet til å skaffe seg innsyn. Hvorvidt det er adgang til å fornye pålegget om 90 dagers lagringsplikt fremstår som uklart. Denne regelen gjelder for spesifiserte data, noe som må bety at de kompetente myndighetene i en stat ikke kan gi en generell ordre om at alle trafikkdata skal lagres i en viss periode. Konvensjonen oppstiller ikke en generell lagringsplikt, og pålegger altså ikke tjenestetilbyderne å registrere data som gjør det mulig for politiet å spore opp brukerne av tjenestene. Avgjørende for hva politiet får tilgang til er også her hva som faktisk blir lagret fra tilbyders side.

Art 17 gir regler for et mer effektivt samarbeid tjenestetilbyderne i mellom og i forhold til politiet. Statene skal etter denne vedta regler som er nødvendig for å sikre at slik hurtig oppbevaring av trafikkdata som art 16 krever, er tilgjengelig uavhengig av om en eller flere teletjenestetilbydere var involvert i overføringen av kommunikasjonen. Videre skal statene sikre at en kompetent myndighet (eller en person denne myndigheten må ha delegert sin kompetanse til) raskt får innsyn i en tilstrekkelig

[81] Sunde

mengde trafikkdata til å kunne identifisere tjenestetilbyderen og ruten kommunikasjonen var overført via.

I tillegg til disse reglene, gir konvensjonen i artiklene 18 – 21 regler om utleveringspålegg, ransaking og beslag i lagrede data, kommunikasjonskontroll i sann tid, og kommunikasjonsavlytting. Slike regler er gjennomført i norsk rett, jf ovenfor avsnitt 4.2.4.4.

Konvensjonen presiserer at den ivaretar respekten for de tradisjonelle rettssikkerhetsgarantier, jf fortalens 10. avsnitt. Den henviser bl a til EMK og FNs konvensjon om sivile og politiske rettigheter, og her særlig til retten til meningsfrihet, ytringsfrihet og privatlivets fred. Denne henvisningen er også gjentatt i art 15, som også slår fast prinsippet om forholdsmessighet. Etter denne skal implementeringen av konvensjonens prosessuelle regler inkludere rettslig eller annen uavhengig kontroll, og det kan settes begrensninger til rekkevidden og varigheten av de prosessuelle virkemidlene. Konvensjonen henviser også til hensynet til personvern, jf henvisningen i fortalens avsnitt 11 til Europarådets konvensjon om beskyttelse av individuelle rettigheter med hensyn til automatisk behandling av personopplysninger.

4.3.4 EMK art 8[82]

Den europeiske menneskerettskonvensjon av 4. november 1950 (EMK) ble implementert som norsk lov ved Lov om styrking av menneskerettighetenes stilling i norsk rett av 21. mai 1999 (menneskerettsloven). Det er konvensjonens artikkel 8 som er relevant i denne sammenheng.

Hovedformålet med art 8 har vært uttrykt som å beskytte individet mot vilkårlig inngrep fra offentlige myndigheter i sitt privatliv eller familieliv[83]. En redegjørelse for bestemmelsens innhold, vil bero på hvordan den er tolket av den europeiske menneskerettsdomstol (EMD). Rettspraksis fra EMD knyttet til art 8 er i stor grad

[82] Fremstillingen her er basert på Bygrave og Møse.

[83] Bygrave s 256

knyttet til de konkrete avgjørelsene, dvs at det i liten grad er gitt generelle uttalelser om hvordan artikkelen skal forstås. Det er derfor nødvendig å gjøre rede for enkeltsaker for å gi et bilde av rettssituasjonen.

Art 8 oppstiller i nr 1 utgangspunktet for individets rettighet: "enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse", deretter følger en opplisting av hvilke forhold som gjør unntak fra dette legitimt. Inngrep som er forbudt etter art 8 (1) rettferdiggjøres under art 8 (2). Vi får her en todelt analyse; først må det vurderes om inngrepet i seg selv er i strid med art 8, og deretter, hvis man konstaterer strid under pkt 1, om det likevel er tillatt fordi det omfattes av unntakene i 2. ledd

Problemstillingen her er hvorvidt EMK art 8 er til hinder for å lagre trafikkdata. De rettigheter slik lagring kan tenkes å være i strid med, er retten til respekt for sitt privatliv og retten til respekt for sin korrespondanse. Vurderingstema er generelt; om regler som pålegger teletjenestetilbyderne lagringsplikt for trafikkdata er i strid med art 8 (1). For å kunne vurdere dette, må innholdet i rettighetene "privatliv" og "korrespondanse" klargjøres. Dette følger av EMDs praksis. Utgangspunktet er at begrepet "privatliv" skal tolkes vidt, og at det ikke kan defineres uttømmende[84]. .

Avlytting av telefoner og registrering av teleopplysninger omfattes av art 8s begreper "privatliv" og "familieliv"[85]. Ved teleopplysning forstås registrering av, hvilke telefoner som har været satt i forbindelse med en bestemt telefon[86]. Begrepet "korrespondanse" omfatter flere måter mennesker kan kommunisere på. I tillegg til "vanlig" korrespondanse via postgang, er også kommunikasjon per telefon, telefaks og e-post inkludert. Straffeprosessuelle tvangsmidler som telefonavlytning og brevkontroll er inngrep som er i strid med retten til respekt for korrespondanse, men kan også ses som et inngrep i den mer generelle retten til respekt for privatliv[87]. (Danelius s 230)

---

[84] Møse s 401

[85] Se Klass m fl v Tyskland pr 41

[86] Se Trier m fl s 247

[87] Danelius s 230.

Den sentrale dommen hva angår trafikkdata er Malone v UK, A 82 (1984). Denne gjaldt kontroll av post, samt avlytting og registrering av telefonsamtaler i forbindelse med at en antikvitetsforhandler var blitt etterforsket for heleri. Domstolen uttalte her at

> "The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts…to an inteference with a right guaranteed by Article 8."

Metering er en benevnelse på registrering av opplysninger om telefonbruk, inkludert de nummer som er oppringt, tidspunkt og varighet på samtalen, men ikke innholdet.

Bygrave[88] finner etter en gjennomgang av relevant rettspraksis at hvorvidt innsamling, registrering eller annen behandling av personopplysninger vil utgjøre et brudd på art 8 (1), avhenger av en rekke momenter, bl a arten av de berørte opplysningene, måten dataene er behandlet på, og i hvilken sammenheng (til hvilket formål (?) opplysningene er samlet. Lagring av trafikkdata vil sannsynligvis bare være i strid med art 8 dersom telefonbrukeren har en rimelig forventning om at slikt ikke forekommer[89].

Den neste problemstillingen er så hvorvidt lagring av trafikkdata kan rettferdiggjøres under art 8 nr 2. For at inngrepet skal kunne rettferdiggjøres under art 8 (2), må tre vilkår være oppfylt: inngrepet må ha hjemmel i lov, det må være nødvendig i et demokratisk samfunn, og det må skje av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter. I denne sammenheng er det særlig hensynet til å forebygge uorden eller kriminalitet som er det aktuelle.

Lovskravet innebærer at det må være et rettslig grunnlag for inngrepet. Det kreves ikke at det skjer med direkte hjemmel i lov; også delegert lovgivning aksepteres. Uttrykket omfatter også rettsregler som er skapt gjennom rettspraksis. Det rettslige grunnlaget må være av en viss kvalitet; det må være tilgjengelig for allmennheten, og tilstrekkelig

---

[88] Bygraves artikkel

[89] Bygraves artikkel s 269.

presist, slik at inngrepet i rettigheten til en viss grad er forutsigbart. Dette betyr bl a at hjemmelen ikke må være for skjønnsmessig utformet. Det sentrale er at individet vernes mot vilkårlig inngrep fra myndighetene. Kravene til hvor klart det rettslige grunnlaget må være, avhenger av hvor alvorlig det påståtte inngrepet er.

Etter gjeldende norsk rett er hjemmel for å lagre trafikkdata gitt i konsesjon fra Datatilsynet til de ulike teletjenestetilbyderne. Dette kan ikke være tilstrekkelig etter EMK art 8; norske borgerne har liten mulighet til å sette seg inn i disse konsesjonsvilkårene, og dermed liten grunn til å forutse at det lagres opplysninger om deres bruk av elektronisk kommunikasjon.

Vilkåret "nødvendig i et demokratisk samfunn" har vært tolket av EMD dit hen at det er oppfylt når inngrepet refererer seg til et "presserende sosialt behov" og er "proporsjonalt i forhold til det legitime formål som forfølges"[90] Se Olsson-dommen A/130 (1988) para 67 uttalte dommen følgende:

> According to the Court's established case-law, the notion of necessity implies that the interferense correspondends to a pressing social need and, in particular, that it is porportionate to the legitimate aim pursued.

Statene er gitt en viss skjønnsmargin for vurdering av hva som er proporsjonalt. Domstolen har fremholdt at inngrep ved bruk av ekstraordinære etterforskningsmetoder likevel kan være proporsjonalt dersom andre, mindre inngripende metoder har vært mislykket eller uanvendelige. Inngrepets omfang må dessuten kunne rettferdiggjøres i forhold til hvor alvorlig det antatte lovbruddet er. Proporsjonalitetsvurderingen skal ta hensyn til den mistenktes rettigheter, men også til andre tredjepersoner som kan bli rammet av tiltaket, f eks familiemedlemmer.[91] Staten gis et rom for en skjønnsmessig vurdering av når disse vilkår er oppfylt. Skjønnsmarginene varierer med ulike forhold; hvor alvorlig inngrepet på den aktuelle rettighet, rettighetens viktighet og hvor viktig det formålet som forfølges er. Statens frihet er likevel ikke ubegrenset, for EMD forbeholder seg retten til å kontrollere om skjønnsfriheten benyttes på en rimelig måte.

---

[90] Leander v Sverige para 58.

[91] Jf Ot prp nr 64 (1998-1999) s

Domstolen har bl a i Malone gitt uttrykk for at kravet til forutberegnelighet ikke skal være så strengt når inngrepet skjer i forbindelse med politiets etterforskning og sikring av nasjonal sikkerhet[92].

Sunde mener at det for norske forhold kun er et spørsmål om lovskravet er oppfylt, da det må være på det rene at inngrepet er nødvendig for å forebygge kriminalitet. Problemstillingen vil da bli hvorvidt art 8 er til hinder for å innføre regler om lagringsplikt for trafikkdata, med det formål at politiet skal kunne bruke det i etter forskningsøyemed.

[92] Bygrave s 271.

5 Avsluttende bemerkninger

Kanskje er det ikke så farlig om man åpner for tilgang til trafikkdata ved etterforskning av den enkelte kriminelle handling, forutsatt at det skjer etter balanserte regler som ivaretar hensynet til personvern. I det enkelte tilfelle er det vanskelig å argumentere for at man ikke skal kunne innhente trafikkdata, særlig dersom dette kan være med på å oppklare en alvorlig kriminell handling. Det kan imidlertid stilles spørsmål til effekten av en eventuell lagringsplikt for trafikkdata. En innvending er at kriminelle kan finne andre måter å kommunisere på, når de ser at trafikkdata blir brukt til oppklaring av kriminelle handlinger.

Elektronisk behandling av data representerer store muligheter for å koble ulike registre med personopplysninger. Det innebærer en latent mulighet for myndighetene til å benytte disse på en annen måte enn opprinnelig forutsatt. Følgelig innebærer det en potensiell fare for misbruk, f eks ved at opplysningene kan bli brukt som et middel til å kontrollere visse grupper av borgerne, med de inngrep på personvernet dette medfører. Det er derfor grunn til bekymring over en internasjonal tendens til å ville innføre lagringsplikt for stadig lengre perioder; i England er det foreslått lagringsplikt på 7 år[93], og Politiets Sikkerhetstjeneste ønsker at det skal være 3-5 års lagring i Norge[94].

[93]

[94] Se Ot prp nr 58 (2002-03).

Litteraturliste

Bøker:

Bygrave, Lee A.:

Data Protection Law; Approaching Its Rationale, Logic and Limits
Kluwer Law International 2002

Personvern i praksis
Cappelen Akademiske Forlag 1997

Bygrave, Lee A og Schartum, Dag Wiese:

Personvern og personopplysningsvern – Innføring i teori og lovgivning
Under publikasjon 2003.

Bing, Jon:

Personvern i faresonen
Cappelen Forlag 1991

Bing, Jon m fl

Innføring i telekommunikasjonsrett
Cappelen Forlag 2001

Bjerke, Hans Kristian og Keiserud, Erik:

Kommentarutgave til straffeprosessloven Bind 1
Universitetsforlaget 2001

Danelius, Hans:

Mänskliga rättigheter i europeisk praxis
En kommentar til Europakonventionen om de mänskliga rättigheterna
Norstedts Juridik AB 1998

Eckhoff, Torstein:

Rettskildelære

4. utgave ved Jan E. Helgesen

Tano Aschehoug 1997

Lenth, Claude A:

Adgangen til å benytte personopplysninger

Complex 2/2000

Lorenzen, Peer, Rehof, Lars Adam og Trier, Tyge:

Den Europæiske Menneskeretskonvention

Jurist- og Økonomforbundets Forlag 1994

Mestad, Ingvild:

Elektroniske spor. Nye perspektiver på personvern

Complex 3/86

Møse, Erik:

Menneskerettigheter

Cappelen Forlag 2002

Wiik Johansen, Kaspersen og Bergseng Skullerud:

Personopplysningsloven, kommentarutgave

Universitetsforlaget 2001

Artikler:

Allitsch, Rainer:

Data Retention on the Internet. A measure with one foot offside?

Computer und Recht International 6/2002

Bygrave, Lee A.:

Data Protection Pusuant to the Right to Privacy in Human Rights Treaties

(International Journal of Law and Information Technology, vol 6 No 3 1998)

Manansian, David:

Digital dilemmas. A survey of the internet society

The Economist 25.01.03

Sunde, Inger Marie:

IKT-kriminalitet: Etterforskningsmetoder og personvern

Tidsskrift for kriminalvitenskap, september 2000.

Convention on cyber crime

Tidsskrift for strafferett 1/2002

(http://www.jus.uio.no/sekr/studieinformasjon/fagsider/spesialoppgave/retningslinjer)